Statement of

Dr. Martin Herman
Chief, Information Access Division
Information Technology Laboratory

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Before the

House of Representatives
Committee on Homeland Security
Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

"Ensuring the Security of America's Borders through the Use of Biometric Passports and other Identity Documents"

June 22, 2005

Chairman Lungren, Ranking Member Sanchez, and members of the Subcommittee, thank you for the opportunity to testify today about the biometric activities of the National Institute of Standards and Technology (NIST) that will help secure America's boarders.

Under the USA Patriot Act (Public Law 107-56) and the Enhanced Border Security and Visa Entry Reform Act (Public Law 107-173), the Attorney General, and the Secretary of State, in consultation with NIST were directed to make recommendations for means of verifying the identity of travelers entering the United States with visas. These recommendations were made in the joint report to Congress entitled "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents," dated February 2003.

Since this report was issued NIST has continued to conduct an extensive biometric research and evaluation program. In particular, NIST is studying three types of biometric technologies: fingerprints, facial recognition, and iris recognition. These three biometrics were specified for international travel documents by the International Civil Aviation Organization (ICAO). ICAO has specified face biometrics as required for such documents, while fingerprints and iris are optional.

NIST, in close collaboration with the Departments of Homeland Security, Justice, Defense, and State has performed many tests of fingerprint and face recognition systems to support its statutory mandates. Fingerprint tests have been performed on the FBI's Integrated Automated Fingerprint Identification System (IAFIS), used to perform criminal background checks; DHS's Automated Biometric Identification System (IDENT), used as part of the US-VISIT system; and many commercial vendor systems. Face recognition tests have been performed on many commercial and academic systems.

To support these tests, NIST has acquired very large sets of data. For example, NIST has obtained 128 million fingerprint images taken from 18 million subjects by several Federal, State and County agencies. This data includes rolled, slap, and flat fingerprints captured either from paper using ink or from live-scan readers. A rolled fingerprint involves capturing the full finger image as it is rolled from one edge of the fingernail to the other. Slap fingerprints involve capturing the four fingers of a hand placed together on a flat surface, followed by a separate capture of the thumb. A flat fingerprint captures the image of only a single finger placed on the surface.

NIST has performed tests of both verification matching and identification. Verification is a one-to-one comparison in which the biometric system attempts to confirm an individual's claimed identity. The individual's biometric information is submitted and compared to an existing template. In US-VISIT, this occurs during the time of border crossing when the system determines whether the person holding the travel document is the same person to whom the document was issued.

Identification is a one-to-many comparison where the biometric system attempts to determine the identity of an individual. An individual's biometric information is collected and compared to all the templates in a database. In US-VISIT, this occurs during the time of enrollment when a person is checked against a watchlist derived in part from the FBI criminal database as well as the IDENT databases. First a database is checked to determine whether the person is on the watchlist. Second a database is checked to ensure that the person has not been previously enrolled in the database under a different name.

NIST's activities require substantial financial and logistical support from external agencies, whom we are fortunate to collaborate with. For example, research and evaluation activities are coordinated through the National Science & Technology Council's Subcommittee on Biometrics. NIST has also been actively working with several standards development organizations in development of fingerprint, face, and iris standards. These organizations include the International Organization for Standardization (ISO), the International Committee for Information Technology Standards (INCITS), and the American National Standards Institute (ANSI).

PATRIOT ACT RECOMMENDATIONS

For one-to-one verification matching, NIST's Patriot Act recommendation is to use one face image and two index finger prints. All three biometrics should be stored in image form. The face image should conform to the ANSI/INCITS 385-2004 standard. The fingerprint images should conform to the ANSI/NIST-ITL 1-2000 standard with 500 dots per inch (dpi) scan resolution.

For one-to-many identification matching, NIST recommends the use of ten slap fingerprint images stored in type 14 ANSI/NIST-ITL 1-2000 formatted records. These 10 fingerprints could be used for enrollment and checking of large databases. This ANSI/NIST standard, entitled "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information," is also used for the electronic exchange of fingerprint images, and is currently used for law enforcement purposes to exchange fingerprints between the FBI and Interpol as well as with the United Kingdom's Home Office.

Face images are not recommended by NIST for large scale applications.

It is important to note that NIST's process for arriving at these recommendations and therefore the recommendations themselves, do not take into account likely impacts of implementing these recommendations on the U.S. economy, international reaction or contemplate the resources necessary to implement.

Again these recommendations were issued in a joint report to Congress. Since this report was issued, NIST has conducted extensive testing of biometric systems that continue to support these recommendations.

VERIFICATION

To verify a person's identity, NIST tests have shown that contemporary fingerprint systems are more accurate than face recognition systems in operational environments. However, this should be qualified by the fact that NIST has not tested facial recognition since the 2002 Face Recognition Vendor Test (FRVT). We believe there have been improvements in facial recognition since then. Department of State, for example, reports having success with facial recognition, both in one-to-one and one-to-many verification, with its Diversity Visa Program and in certain nonimmigrant visa applications. Also the Face Recognition Grand Challenge, a development effort funded by multiple federal agencies and managed by NIST, aims to reduce the error rate by and order of magnitude over these levels. Preliminary results show that the community has met this goal in laboratory environments, but a definitive answer will not be available until completion of FRVT 2005.

Based on what we found in 2002, the two-fingerprint probability of verification (or true accept rate, TAR) for the US-VISIT two-fingerprint matching system is 99.6 while the best 2002 face recognition probability of verification was 90 percent using a single face image with controlled illumination. (Controlled illumination involves controlled light sources that illuminate the face while taking the picture). Additional FRVT 2002 results show that face recognition performance decreases significantly under uncontrolled conditions; the best probability of verification was 54 percent when using outdoor illumination. Currently in the US-VISIT system, illumination is uncontrolled when face images are obtained. Based on the 2002 data, even under controlled illumination, the error rate of face recognition is 25 times higher than the two-fingerprint results. Clearly, for the current US-Visit implementation, two fingerprints are much better solution than a single uncontrolled face image.

IDENTIFICATION

For identification applications, extensive testing by NIST of commercial fingerprint systems has confirmed the requirement for ten slap fingerprints. During the Fingerprint Vendor Technology Evaluation, 2003, again funded by multiple federal agencies and managed by NIST, eighteen different companies' products were tested, and thirty-four systems were evaluated. Different data subtests measured accuracy for various numbers and types of fingerprints, using operational fingerprint data from a variety of U.S. Government sources. 48,105 sets of fingerprints (393,370 distinct fingerprint images) from 25,309 individuals were used for analysis.

For all systems tested, the accuracy increases as the number of fingers increase. The improvement is both large and consistent. Although the actual benefits were found to vary by dataset and by system, the general trend was quite consistent. The accuracy of searches using four or more fingers was higher than the accuracy of two-finger searches, which was higher than the accuracy of single-finger searches.

These results are strongly dependent on fingerprint image quality. For the US-VISIT fingerprint matching system, using Department of State (DOS) Mexican visa Border Crossing Card (BCC) data, the probability of identification (or true accept rate, TAR) using index finger pairs is independent of background database size over the range from 100,000 entries to 6,000,000 entries. Using the operational thresholds, the probability of identification is 96 percent. If, however, fingerprint quality rather that database size is the controlling factor, then for low-quality data, the probability of identification falls to 53.6 percent. With high quality fingerprint images, the probability of identification is 99.6 percent. Image quality is important since the fingerprint quality of most archival law enforcement databases is lower than the quality of the data presently being collected by US-VISIT and will remain so for some time into the future. The only tested method for improving matching accuracy for databases with lower image quality is to increase the number of fingers used. When 10-fingers are used, the probability of identification for the most accurate commercial system tested exceeded 99.95 percent, with a false accept rate (FAR) of 0.01 percent.

Details for all the results described here can be obtained at http://www.itl.nist.gov/iad/894.03/pact/pact.html.

IRIS

Iris recognition is a potentially valuable technology that needs considerably more testing to determine its accuracy in operational environments. A recent non-NIST study of iris recognition has shown failure-to-enroll rates of about 2 percent. This means that 2 percent of the time, the system cannot perform an iris match. Fingerprints have close to zero failure-to-enroll rates. NIST is planning an iris data collection effort using 10,000 individuals over the next year to obtain a vendor-neutral data set in operational environments. This plus other large-scale data sets will then be used to perform iris recognition tests over the next two years.

CONCLUSION

As the Committee can see, NIST, in close partnership with federal sponsors and partners, has a vibrant biometrics program in the areas of fingerprint and facial recognition, and is also planning activities in the area of iris recognition. NIST tests have demonstrated that fingerprints are significantly more accurate than facial recognition for current US-VISIT applications, while iris recognition needs further assessment.

Thank you for the opportunity to testify. I would be happy to answer any questions the Committee might have.